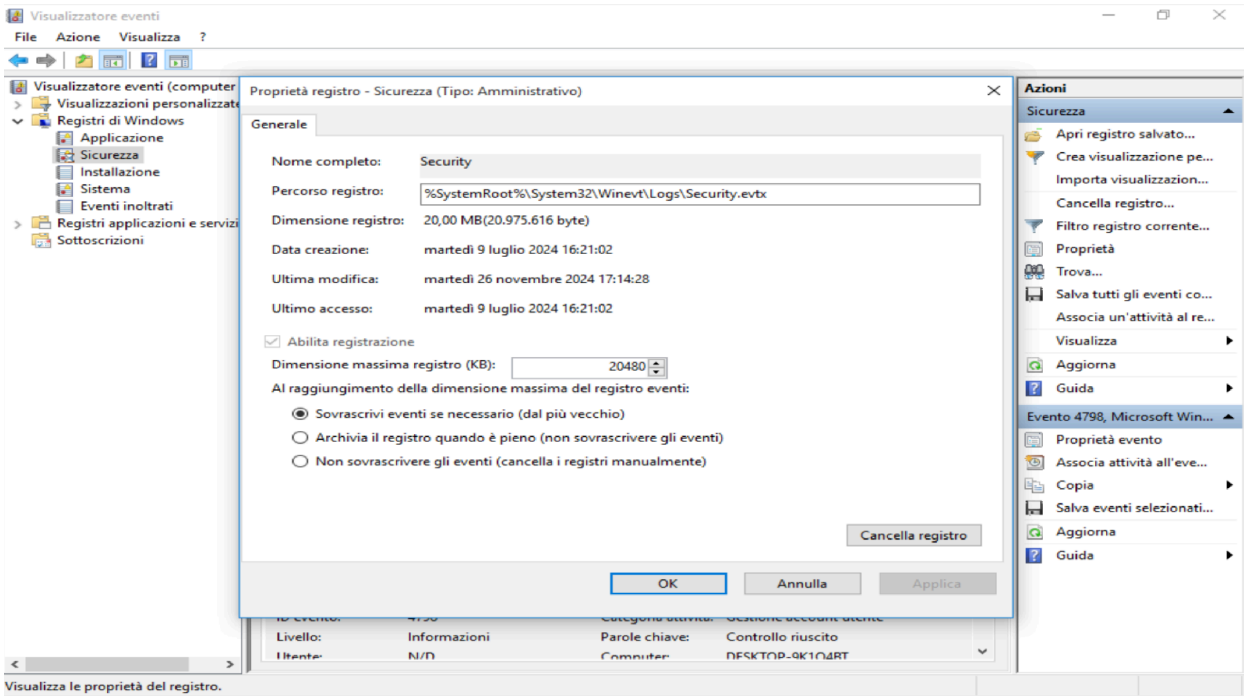
Esercizio di oggi:
Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

Obiettivo:
Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.

Istruzioni:

- 1. Accedere al Visualizzatore Eventi:
  - Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
  - Digita eventvwr e premi Invio.
- 2. Configurare le Proprietà del Registro di Sicurezza:
  - Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".



Oggi abbiamo visto le funzioni principali del SOC (cioè team che si occupa di prevenzione quotidiana nel campo del lavoro) che attraverso il SIEM monitora e gestisce i file che danno informazioni sulla sicurezza come i file di log e abbiamo visto anche l'introduzione del SOAR (macchina che rende questi sistemi di prevenzione e cura dei danni automatici).

In un SOC (Security Operations Center), i file di log svolgono un ruolo cruciale nella protezione della rete, sistemi e applicazioni di una organizzazione. Si tratta di registrazioni dettagliate delle attività e degli eventi che avvengono all'interno di una infrastruttura IT. Una delle funzioni principali dei file di log in un SOC è quella di monitorare in tempo reale le attività all'interno dell'infrastruttura IT. I dati contenuti nei file di log sono: tentativi di accesso, modifiche ai file di sistema, movimenti di rete (connessioni in ingresso ed uscita), errori di sistema o delle

applicazioni. I file di log possono individuare dati come accessi non autorizzati, anomalie di traffico o modifiche inaspettate. Aiutano nella rilevazione precoce di potenziali minacce e nell’evitamento di incidenti informatici.